

Title (en)
SECURE COMMUNICATION

Title (de)
SICHERE KOMMUNIKATION

Title (fr)
COMMUNICATION SÉCURISÉE

Publication
EP 2859679 B1 20200902 (EN)

Application
EP 13725454 A 20130523

Priority
• GB 201209286 A 20120523
• GB 201209308 A 20120523
• GB 2013051361 W 20130523

Abstract (en)
[origin: WO2013175224A1] A method for allowing a first party and a second party to obtain shared secret information is provided. The method comprises the steps of: obtaining, by the first party, a sequence of values $A=X+N$ A where X is a sequence of values and N A is a random sequence associated with the first party; obtaining, by the second party, a sequence of values $B=X+N$ B where N B is a random sequence associated with the second party; performing, by the first and second parties, a data matching procedure to identify corresponding pairs of values, $\langle u \rangle a \langle u \rangle \langle u \rangle j \langle u \rangle$, $\langle u \rangle b \langle u \rangle \langle u \rangle j \langle u \rangle$, in respective sequences $\langle u \rangle A \langle u \rangle$ and $\langle u \rangle B \langle u \rangle$ that match, wherein sequences $\langle u \rangle A \langle u \rangle$ and $\langle u \rangle B \langle u \rangle$ are discrete-valued sequences equal to, derived from, or derived using, sequences A and B; wherein the shared secret information is equal to, or derived from, or derived using, the matching values in sequences A and B.

IPC 8 full level
H04L 9/08 (2006.01)

CPC (source: EP KR US)
H04L 9/08 (2013.01 - KR); **H04L 9/0816** (2013.01 - KR); **H04L 9/0852** (2013.01 - EP US); **H04L 9/0858** (2013.01 - EP US);
H04L 9/0838 (2013.01 - EP US)

Citation (examination)
WALLACE J: "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits", COMMUNICATIONS, 2009. ICC '09. IEEE INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 14 June 2009 (2009-06-14), pages 1 - 5, XP031506414, ISBN: 978-1-4244-3435-0

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)
WO 2013175224 A1 20131128; AU 2013265020 A1 20150122; AU 2013265020 B2 20171012; CN 104412538 A 20150311;
CN 104412538 B 20190409; EP 2859679 A1 20150415; EP 2859679 B1 20200902; JP 2015522998 A 20150806; KR 20150031245 A 20150323;
US 10009175 B2 20180626; US 2015134947 A1 20150514

DOCDB simple family (application)
GB 2013051361 W 20130523; AU 2013265020 A 20130523; CN 201380035492 A 20130523; EP 13725454 A 20130523;
JP 2015513272 A 20130523; KR 20147036225 A 20130523; US 201314403144 A 20130523